A note on primes in certain residue classes

International Journal of Number Theory

A note on primes in certain residue classes

Paolo Leonetti
Department of Statistics, Università "Luigi Bocconi"
Via Roberto Sarfatti 25, 20100 Milano, Italy
leonetti.paolo@gmail.com

Carlo Sanna
Department of Mathematics, Università degli Studi di Torino
Via Carlo Alberto 10, 10123 Torino, Italy
carlo.sanna.dev@gmail.com

Received (Day Month Year)
Accepted (Day Month Year)

Given positive integers $a_1, \ldots, a_k$, we prove that the set of primes p such that $p \not\equiv 1 \bmod a_i$ for $i = 1, \ldots, k$ admits asymptotic density relative to the set of all primes which is at least $\prod_{i=1}^{k} \left(1 - \frac{1}{\varphi(a_i)}\right)$, where φ is the Euler totient function. This result is similar to the one of Heilbronn and Rohrbach, which says that the set of positive integer n such that $n \not\equiv 0 \bmod a_i$ for $i = 1, \ldots, k$ admits asymptotic density which is at least $\prod_{i=1}^{k} \left(1 - \frac{1}{a_i}\right)$.

Keywords: congruences; densities; primes in residue classes; set of multiples.

Mathematics Subject Classification 2010: 11N13, 11N05, 11N69.

1. Introduction

The *natural density* of a set of positive integers $\mathcal{A}$ is defined as

$$\mathbf{d}(\mathcal{A}) := \lim_{x \to +\infty} \frac{\#(\mathcal{A} \cap [1, x])}{x},$$

whenever this limit exists. The study of natural densities of sets of positive integers satisfying some arithmetic constraints is a classical research topic. In particular, Heilbronn [10] and Rohrbach [11] proved, independently, the following result:

Theorem 1.1. *Let $a_1, \ldots, a_k$ be some positive integers. Then, the set $\mathcal{A}$ of positive integers n such that $n \not\equiv 0 \bmod a_i$ for $i = 1, \ldots, k$ has natural density satisfying*

$$\mathbf{d}(\mathcal{A}) \geq \prod_{i=1}^{k} \left(1 - \frac{1}{a_i}\right).$$

Generalizations of Theorem 1.1 were given, for instance, by Behrend [3] and Chung [5]. We refer to [9] for a textbook exposition and to [1,2,8,12] for related results. It is worth noting that Besicovitch [4] proved that, given a sequence of positive integers $(a_i)_{i\geq 1}$, the set $\mathcal{A}$ of positive integers n not divisible by any a_i does not necessarily admit natural density. However, Davenport and Erdős [6] proved that $\mathcal{A}$ always admits logarithmic density, i.e., the following limit exists:

$$\lim_{x\to+\infty} \frac{1}{\log x} \sum_{n\in\mathcal{A}\cap[1,x]} \frac{1}{n}.$$

The purpose of this note is to prove a result for the set of primes analogous to Theorem 1.1. Of course, to this aim, the natural density is not the right quantity to consider, since it is well known that the set of primes has natural density equal to zero.

Define the *relative density* of a set of primes $\mathcal{P}$ to be

$$\mathbf{r}(\mathcal{P}) := \lim_{x\to+\infty} \frac{\#(\mathcal{P}\cap[1,x])}{x/\log x},$$

whenever this limit exists. Furthermore, let φ denote the Euler totient function.

Our result is the following:

Theorem 1.2. *Let $a_1,\dots,a_k$ be positive integers. Then the set $\mathcal{P}$ of primes p such that $p\not\equiv 1 \bmod a_i$ for $i=1,\dots,k$ has relative density satisfying*

$$\mathbf{r}(\mathcal{P}) \geq \prod_{i=1}^{k}\left(1-\frac{1}{\varphi(a_i)}\right).$$

2. Preliminaries

We begin by fixing some notations with the aim of simplifying the exposition. Let $\mathbf{N}$ be the set of positive integers. Put $[\![x,y]\!] := [x,y]\cap\mathbf{N}$ for all $x\leq y$, and let the other "integral interval" notations, like $]\!]x,y]\!]$, be defined in the obvious way. For vectors $\mathbf{x}=(x_1,\dots,x_d)$ and $\mathbf{y}=(y_1,\dots,y_d)$ belonging to $\mathbf{N}^d$, define $\|\mathbf{x}\| := x_1\cdots x_d$ and $[\![\mathbf{x},\mathbf{y}]\!] := [\![x_1,y_1]\!]\times\cdots\times[\![x_d,y_d]\!]$. Also, all the elementary operations of addition, subtraction, multiplication, and division between vectors are meant to be component-wise, e.g., $\mathbf{xy} := (x_1y_1,\dots,x_dy_d)$. Let $\mathbf{0}$, respectively $\mathbf{1}$, be the vector of $\mathbf{N}^d$ with all components equal to 0, respectively 1, where d will be always clear from the context. Finally, write $\mathbf{x}\equiv\mathbf{y} \bmod \mathbf{m}$ if and only if $x_i\equiv y_i \bmod m_i$ for all $i=1,\dots,d$, where $\mathbf{m}=(m_1,\dots,m_d)\in\mathbf{N}^d$, and write $\mathbf{x}\not\equiv\mathbf{y} \bmod \mathbf{m}$ if and only if $x_i\not\equiv y_i \bmod m$ for at least one $i\in[\![1,d]\!]$.

We will need the following lemma, which might be interesting per se.

Lemma 2.1. *Let d be a positive integer and let $\mathbf{a}_1,\dots,\mathbf{a}_k,\mathbf{b}\in\mathbf{N}^d$ be vectors such that $\mathbf{a}_1\cdots\mathbf{a}_k\equiv\mathbf{0} \bmod \mathbf{b}$ and $\mathbf{b}\equiv\mathbf{0} \bmod \mathbf{a}_i$ for $i=1,\dots,k$. Then the set $\mathcal{X}$ of all*

$\mathbf{x} \in [\![\mathbf{1}, \mathbf{b}]\!]$ *such that* $\mathbf{x} \not\equiv \mathbf{0} \bmod \mathbf{a}_i$ *for* $i = 1, \dots, k$ *satisfies*

$$\#\mathcal{X} \geq \|\mathbf{b}\| \cdot \prod_{i=1}^{k} \left(1 - \frac{1}{\|\mathbf{a}_i\|}\right).$$

Proof. Define $\mathbf{c} := \mathbf{a}_1 \cdots \mathbf{a}_k$ and let $\mathcal{Y}$ be the set of $\mathbf{y} \in [\![\mathbf{1}, \mathbf{c}]\!]$ such that $\mathbf{y} \not\equiv \mathbf{0} \bmod \mathbf{a}_i$ for $i = 1, \dots, k$. Then, a result of Chung [5] says that

$$\#\mathcal{Y} \geq \|\mathbf{c}\| \cdot \prod_{i=1}^{k} \left(1 - \frac{1}{\|\mathbf{a}_i\|}\right). \tag{2.1}$$

Clearly, $\mathcal{Y}$ can be partitioned in $\|\mathbf{c}/\mathbf{b}\|$ sets given by

$$\mathcal{Y}_{\mathbf{t}} :=]\!]\mathbf{b}(\mathbf{t} - \mathbf{1}), \mathbf{bt}]\!] \cap \mathcal{Y},$$

for $\mathbf{t} \in [\![\mathbf{1}, \mathbf{c}/\mathbf{b}]\!]$. (Note that $\mathbf{c}/\mathbf{b} \in \mathbf{N}^d$ since $\mathbf{a}_1 \cdots \mathbf{a}_k \equiv \mathbf{0} \bmod \mathbf{b}$.) Therefore, by (2.1) there exists some $\mathbf{t} \in [\![\mathbf{1}, \mathbf{c}/\mathbf{b}]\!]$ such that

$$\#\mathcal{Y}_{\mathbf{t}} \geq \frac{\#\mathcal{Y}}{\|\mathbf{c}/\mathbf{b}\|} \geq \|\mathbf{b}\| \cdot \prod_{i=1}^{k} \left(1 - \frac{1}{\|\mathbf{a}_i\|}\right).$$

Moreover, for each $\mathbf{y} \in \mathcal{Y}_{\mathbf{t}}$ there exists a unique $\mathbf{x} \in [\![\mathbf{1}, \mathbf{b}]\!]$ such that $\mathbf{x} \equiv \mathbf{y} \bmod \mathbf{b}$. Finally, since $\mathbf{b} \equiv \mathbf{0} \bmod \mathbf{a}_i$ for $i = 1, \dots, k$, it follows easily that the map $\mathbf{y} \mapsto \mathbf{x}$ is an injection $\mathcal{Y}_{\mathbf{t}} \to \mathcal{X}$, so that $\#\mathcal{X} \geq \#\mathcal{Y}_{\mathbf{t}}$ and the proof is complete. □

We will also use the following version of Dirichlet's theorem on primes in arithmetic progressions [7, pag. 82].

Theorem 2.2. *For all coprime positive integers* a *and* b*, the set of primes* p *such that* $p \equiv a \bmod b$ *has relative density equal to* $1/\varphi(b)$.

3. Proof of Theorem 1.2

Put $\ell := \operatorname{lcm}(a_1, \dots, a_k)$ and let $\ell = p_1^{e_1} \cdots p_d^{e_d}$ be the canonical prime factorization of ℓ, where $p_1 < \cdots < p_d$ are primes and $e_1, \dots, e_d$ are positive integers. Furthermore, let $\mathcal{S}$ be the set of all $n \in [\![1, \ell]\!]$ such that: n is relatively prime to ℓ, and $n \not\equiv 1 \bmod a_i$ for $i = 1, \dots, k$. Thanks to Theorem 2.2, we have

$$\mathbf{r}(\mathcal{P}) = \lim_{x \to +\infty} \frac{\#(\mathcal{P} \cap [1, x])}{x/\log x} = \lim_{x \to +\infty} \sum_{n \in \mathcal{S}} \frac{\#\{p \leq x : p \equiv n \bmod \ell\}}{x/\log x} = \frac{\#\mathcal{S}}{\varphi(\ell)}, \tag{3.1}$$

hence the relative density of $\mathcal{P}$ exists, and all we need is the right lower bound for $\#\mathcal{S}$.

For the sake of clarity, let us first assume that $8 \nmid \ell$. Later, we will explain how to adapt the proof for the case $8 \mid \ell$. Let g_i be a primitive root modulo $p_i^{e_i}$, for $i = 1, \dots, d$. Note that g_1 exists when $p_1 = 2$ since $e_1 \leq 2$. Put also $\mathbf{b} := (\varphi(p_1^{e_1}), \dots, \varphi(p_d^{e_d}))$. By the Chinese Remainder Theorem, each $n \in [\![1, \ell]\!]$ which is relatively prime to ℓ is uniquely identified by a vector

$\mathbf{x}(n) = (x_1(n), \dots, x_d(n)) \in [\![\mathbf{1}, \mathbf{b}]\!]$ such that $n \equiv g_i^{x_i(n)} \bmod p_i^{e_i}$ for $i = 1, \dots, d$. Let $a_i = p_1^{\alpha_{i,1}} \cdots p_d^{\alpha_{i,d}}$ be the prime factorization of a_i, where $\alpha_{i,1}, \dots, \alpha_{i,d}$ are nonnegative integers, and define $\mathbf{a}_i := (\varphi(p_1^{\alpha_{i,1}}), \dots, \varphi(p_d^{\alpha_{i,d}}))$ for $i = 1, \dots, k$.

At this point, it follows easily that $n \in \mathcal{S}$ if and only if $\mathbf{x}(n) \in \mathcal{X}$, where $\mathcal{X}$ is the set in the statement of Lemma 2.1. Hence, the map $n \mapsto \mathbf{x}(n)$ is a bijection $\mathcal{S} \to \mathcal{X}$ and, as a consequence, $\#\mathcal{S} = \#\mathcal{X}$. Since $\|\mathbf{b}\| = \varphi(\ell)$, $\|\mathbf{a}_i\| = \varphi(a_i)$, $\mathbf{a}_1 \cdots \mathbf{a}_k \equiv \mathbf{0} \bmod \mathbf{b}$, and $\mathbf{b} \equiv \mathbf{0} \bmod \mathbf{a}_i$ for $i = 1, \dots, k$, the desired claim follows from Lemma 2.1 and (3.1).

The case $8 \mid \ell$ is a bit more trickier since there are no primitive roots modulo 2^e, for $e \geq 3$ an integer. However, the previous proof still works by putting

$$\mathbf{b} := (2, 2^{e_1-2}, \varphi(p_2^{e_2}), \dots, \varphi(p_d^{e_d}))$$

and

$$\mathbf{a}_i := (2^{\max(0,\alpha_{i,1}-1)-\max(0,\alpha_{i,1}-2)}, 2^{\max(0,\alpha_{i,1}-2)}, \varphi(p^{\alpha_{i,2}}), \dots, \varphi(p^{\alpha_{i,d}}))$$

for $i = 1, \dots, k$. Now each $n \in [\![1, \ell]\!]$ which is relatively prime to ℓ is uniquely identified by a vector $\mathbf{x}(n) = (x_0(n), \dots, x_d(n)) \in [\![\mathbf{1}, \mathbf{b}]\!]$ such that $n \equiv (-1)^{x_0(n)} 5^{x_1(n)} \bmod 2^{e_1}$ and $n \equiv g_i^{x_i(n)} \bmod p_i^{e_i}$ for $i = 2, \dots, d$. The rest of the proof proceeds as before.

Acknowledgments

The authors thank the anonymous referee for carefully reading the paper.

References

[1] R. Ahlswede and L. H. Khachatrian, *Density inequalities for sets of multiples*, J. Number Theory **55** (1995), no. 2, 170–180.
[2] R. Ahlswede and L. H. Khachatrian, *Number-theoretic correlation inequalities for Dirichlet densities*, J. Number Theory **63** (1997), no. 1, 34–46.
[3] F. A. Behrend, *Generalization of an inequality of Heilbronn and Rohrbach*, Bull. Amer. Math. Soc. **54** (1948), 681–684.
[4] A. S. Besicovitch, *On the density of certain sequences of integers*, Math. Ann. **110** (1935), no. 1, 336–341.
[5] K.-L. Chung, *A generalization of an inequality in the elementary theory of numbers*, J. Reine Angew. Math. **183** (1941), 193–196.
[6] H. Davenport and P. Erdős, *On sequences of positive integers*, J. Indian Math. Soc. (N.S.) **15** (1951), 19–24.
[7] M. Ch.-J. de la Vallée Poussin, *Recherches analytiques sur la théorie des nombres premiers*, Hayez, Imprimeur de L'Académie Royale de Belgique, Bruxelles, 1897.
[8] P. Erdős, *On the density of some sequences of integers*, Bull. Amer. Math. Soc. **54** (1948), 685–692.
[9] R. R. Hall, *Sets of multiples*, Cambridge Tracts in Mathematics, vol. 118, Cambridge University Press, Cambridge, 1996.
[10] H. A. Heilbronn, *On an inequality in the elementary theory of numbers*, Proc. Cambridge Philos. Soc. **33** (1937), 207–209.

[11] H. Rohrbach, *Beweis einer zahlentheoretischen Ungleichung*, J. Reine Angew. Math. **177** (1937), 193–196.
[12] I. Z. Ruzsa, *Probabilistic generalization of a number-theoretical inequality*, Amer. Math. Monthly **83** (1976), no. 9, 723–725.